UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,434	04/22/2005	Unho Choi	5835-001/NP	9122

27572 7590 10/14/2009

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
10/14/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/532,434	CHOI, UNHO	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-74* is/are pending in the application.

4a) Of the above claim(s) *49-74* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **8/14/09** has been entered.

Claims 1-27 have been canceled. Claims 28-74 have been added. Claims 28-48 have been elected by original presentation. Claims 49-74 have been withdrawn from consideration.

Response to Amendment

Election/Restrictions

Restriction is required under 35 U.S.C. 121 and 372.

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1.

Group 1, claim(s) 28-48, drawn to collecting information, simulating threats, and assessing the results of the simulation.

Group 2, claim(s) 49-58, drawn to assessing and sharing threat incidents.

Group 3, claim(s) 59-68, drawn to damage calculations on threat incidents.

Group 4, claim(s) 69-74, drawn to generating risk levels of asset values.

The inventions listed as Groups 1-4 do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

Group 1's special technical feature is to assess the security incidents based on the simulation. Groups 1 lacks the special technical features found in groups 2-4.

Group 2's special technical feature is evaluating and classifying security information related to security incidents. Group 2 lacks the special technical features found in groups 1, 3, and 4.

Group 3's special technical feature is determining an asset value for a computer device. Group 3 lacks the special technical features found in groups 1, 2, and 4.

Group 4's special technical feature is generating a risk level for a computing system based on the simulation of an attack. Group 3 lacks the special technical features found in groups 1-3.

Election by Original Presentation

Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 49-74 are withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

Claim Objections

Claim 43 is objected to because of the following informalities: claim 43 is a duplication of claim 42 with the same dependency to claim 41. Claim 43 should be canceled. Appropriate correction is required.

Response to Arguments

Applicant's arguments with respect to claims 28 and 38 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 28-30, 33-40, and 44-48 are rejected under 35 U.S.C. 102(e) as being anticipated by USP 7,325,252 to Bunker et al., hereinafter Bunker.

As per claims 28 and 38, Bunker teaches a computer emergency response system linked to a plurality of computer systems, the system comprising:

an information section configured to collect system information for at least one of the plurality of computer systems and security information related to one or more security incidents that are a threat to at least one of the plurality of computer systems (col. 3, lines 24-28);

a test bed configured to perform a simulation under a similar condition of at least one of the plurality of computer systems based on the system information and security information (col. 4, lines 5-15); and

an assessment section configured to assess the one or more security incidents based on the simulation (col. 4, lines 17-30).

As per claims 29 and 39, Bunker teaches the test bed resides on a different computer system than the at least one simulated computer system (col. 3, line 65).

As per claims 30 and 40, Bunker teaches the assessment section assesses the one or more security incidents by classifying the one or more security incidents into one or more levels of attack (col. 4, lines 50-55).

As per claims 33 and 44, Bunker teaches the assessment section is further configured to provide a possible scenario for an attack on at least one of the plurality of computer systems (col. 4, lines 60-65).

As per claims 34 and 45, Bunker teaches the assessment section is further configured to use the test bed to automatically assess the one or more security incidents (col. 4, lines 17-21).

As per claims 35 and 46, Bunker teaches an information sharing section configured to classify the security information and transfer the classified security information to at least one of the plurality of computer systems (col. 4, lines 60-65).\

As per claims 36 and 47, Bunker teaches a warning section configured to issue an alert to the simulated computer system based on an assessment of the one or more security incidents by the assessment section (col. 4, line 60).

As per claims 37 and 48, Bunker teaches a warning section configured to issue a forecast to the simulated computer system based on an assessment of the one or more security incidents by the assessment section (col. 4, lines 60-65 and col. 5, line 5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 30, 31, 41, 42, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bunker in view of USP Application Publication 2002/0199122 to Davis et al., hereinafter Davis.

As per claims 31 and 41, Bunker is silent in explicitly disclosing an evaluation section configured to calculate expected damages from an attack based on at least one security incident with a similar level of attack. Bunker teaches many types of threat assessments and generating details analysis of those threats to the system. Davis teaches an evaluation section configured to calculate expected damages from an attack based on at least one security incident with a similar level of attack (0025 and 0033). This detailed report is just another analysis of the potential a threat may incur to a system. This claim would have been obvious because substituting known method with produce predictable results without changing the original intention is within the ordinary capabilities of one of ordinary skill in the art. Substituting or adding another type of assessment to the vulnerability report is obvious.

As per claims 32, 42, and 43, Bunker is silent in explicitly teaching an asset recovery section configured to provide an expected recovery time from the attack for at least one of the plurality of computer systems. Bunker teaches many types of threat assessments and generating details analysis of those threats to the system. Davis

teaches an asset recovery section configured to provide an expected recovery time from the attack for at least one of the plurality of computer systems (0025 and 0033) as being able to determine the elapsed time between when a vulnerability was introduced and the time a solution was fixed. Adding this into the report is yet another assessment detail which would provide a network administrator valuable knowledge pertaining to vulnerability assessment. Examiner supplies the same rationale to combine Bunker and Davis as recited in the rejection of claims 31 and 41. Substituting or adding another type of assessment to the vulnerability report is obvious.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431